STATE OF MINNESOTA)
) ss. AFFIDAVIT OF KATHERINE WESPETAL
COUNTY OF RAMSEY) (correcting paragraphs 29 and 57)

I, Katherine Wespetal, being duly sworn, depose and state as follows:

1. I am a Special Agent ("SA") of the United States Secret Service ("USSS"), and have been for approximately seven years. I am currently assigned to the Minneapolis Field Office. Among my duties as an SA, I am charged with the investigation of financial crimes, including check fraud, identity fraud, credit card fraud, bank and wire fraud and the manufacturing, possession, and passing of counterfeit United States currency. In addition I have received extensive training in Network Intrusion Investigations (Cyber Crime) and am currently assigned to the Minnesota Cyber Crimes Task Force. Over the course of my career I have investigated many sophisticated and organized fraud rings involved in various fraudulent activities. I have become knowledgeable in the ways that individuals commit fraudulent activities and quickly move to launder the proceeds of their criminal activity in an effort to thwart investigative efforts, as well as to hide the proceeds of such activity. I have also investigated many complex, international computer intrusions. These include intrusions into the computers of financial institutions as well as other private industry computers on which financial information is stored.

2. This investigation is being conducted jointly by the United States Secret Service, the Internal Revenue Service – Criminal Investigation Division, and the Minnesota Financial Crimes Task Force. Information obtained as a result of the investigative efforts of each agency is being shared with agents from each of the other agencies, to the extent permitted by law and rule. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other law enforcement officers, review of documents and computer records related

to this investigation, communications with others who have personal knowledge of the events and circumstances described in this affidavit (including participants), and information gained through my training and experience and the training and experience of others.

3. This affidavit is being submitted in support of an application for search warrants for the following sites, including computers, computer peripherals, and storage devices at these sites:

a. Suites 106A and 145, 250 Second Avenue South, Minneapolis, Minnesota.

b. Suite 10, 411 Washington Avenue North, Minneapolis, Minnesota.

c. Suites 210 and 104, 77 13th Avenue Northeast, Minneapolis, Minnesota.

These locations are all associated with STEVEN MARK RENNER and various companies he operates. Your affiant respectfully submits that the facts set out in this affidavit show that there is probable cause to believe that Renner is operating a large, Internet-based, Ponzi scheme through his umbrella corporation, InterMark, and some of its subsidiaries, particularly Virtual Payment Systems, V-Media, Cash Cards International, and V-Local. The primary vehicle for the perpetration of this fraud is called "iNetGlobal," which, appears to be, from documents your affiant has reviewed from the Nevada Secretary of State's Office, incorporated in Nevada. Those documents show the incorporation of the similarly-named "INet Global Productions." The commission by Renner of the federal crimes of wire fraud, in violation of Title 18, United States Code Section 1343, and money laundering, in violation of Title 18, United States Code Section 1957, is essential to the operation of this Ponzi scheme.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation in this

affidavit. Rather, this affidavit only includes the information necessary to show that probable cause exists for search warrants to be issued for the offices, computer workspaces, computers and associated peripherals listed in this affidavit, for the evidence, instrumentalities, and fruits of wire fraud and money laundering listed in the “list of items to be seized.”

Background - Renner

5. Based on my training and experience, I know that computers are frequently used to perpetrate fraud schemes and that several different types of fraud schemes have successfully been perpetrated over the Internet, including, most pertinently to this matter, Ponzi schemes. Ponzi schemes promote allegedly lucrative business opportunities, often involving such exotic money-making enterprises as arbitraging foreign currency exchange rates, trading precious metals, or other high-return investments. But in a Ponzi scheme, there is no underlying profitable business to support the payments promoters say they will make to investors. Instead, the promoters simply use the money obtained from a growing base of later investors to pay so-called "profits" to earlier investors. Schemes that depend on growing the base of new victims to make payments to prior participants are sometimes also referred to as pyramids. The Internet is increasingly used as a vehicle to promote Ponzi schemes..

6. Ponzi schemes have evolved with the development of the Internet, but their basic premise remains the same; later investors’ funds are used to pay the earlier investors. A version of the Ponzi scheme that law enforcement officials have encountered in recent years and that is being used in this case is referred to as an "auto-surf program." "Auto-surf" claims to be a form of online advertising program that generates revenue from so called "advertisers" who pay a membership fee to have their website displayed on the "host's" webpage. As part of the program and to encourage more "advertisers" to pay the membership fee, the "host" pays the "advertisers"

a "rebate" each time they view a webpage of a fellow "advertiser." Increasing the number of times a webpage is viewed is important to someone who advertises on that webpage because the more people who view the webpage, the greater the number of potential customers who are viewing an advertisement for a product or service; and it is important to the person or business whose webpage is hosting the advertising, because frequently the rate charged for advertising is driven, at least in part, by the number of visits made to a website. In the auto-surf Ponzi schemes with which your affiant is familiar, the host encourages "advertisers" to recruit new "advertisers" by paying existing "advertisers" a referral fee for each new “advertiser” they sign up. In this model, the host generates most, if not all, of its revenue from membership fees, not from sales of legitimate advertising services, and therefore must use money received from later "advertisers" to pay "rebates" and referral fees to earlier "advertisers." These programs collapse when membership fees from new "advertisers" are no longer sufficient to cover the payouts promised to existing “advertisers.”

7. There have been at least three earlier examples of “autosurf” Ponzi schemes of which your affiant is aware. In early 2006, the United States Securities and Exchange Commission ("SEC") successfully sued an Internet-based auto-surf Ponzi operation named “12daily Pro.” According to the SEC's Complaint, 12daily Pro purported to be a "paid Autosurf program" whereby members would earn money for "viewing the websites owned or promoted by other online professionals." As described by the SEC in its Complaint, members purportedly paid money (membership fees) to 12daily Pro (the host) in return for which 12daily Pro promised to pay its members to view advertisers’ rotating websites. Although the operators of 12daily Pro purported to be paying members from earnings that were "financed by multiple income streams, including advertising and off-site investments," the SEC's investigation

determined that almost all of the funds that the operators paid to members came from the membership fees paid by other members. The operators of 12daily Pro did not generate any significant independent revenue to support the payouts it promised to its membership. Instead, it operated as a pure Ponzi scheme that could not sustain its promised payments absent an ever-increasing number of new or upgraded members. The SEC estimated that before it successfully intervened the operators of 12daily Pro took in over $50 million from approximately 300,000 "investors" nationwide and overseas.

8. In July 2007, the SEC successfully sued the operators of another Internet-based auto-surf Ponzi scheme, known as “Phoenixsurf,” that offered “investors” a 120% return in just 8 days on investments ranging from $8 to $6,000. To receive the promised returns, the investors had to purchase advertising and view at least 15 webpages of advertising per day during the 8-day period. Although the website operators represented that they would pay the promised returns with funds received from other businesses and programs within its network, the SEC charged the operators with operating Phoenixsurf.com “primarily as a pure Ponzi scheme – using for the most part only new investor funds to pay the promised returns to existing investors.” In its Complaint, the SEC alleged that, during its operation, this Ponzi scheme paid to the earlier investors $36.7 million of the $41.9 million it raised, leaving $5.2 million unaccounted-for.

9. In July 2008, the US Secret Service investigated the operators of yet another Internet-based auto-surf Ponzi scheme, known by various names, including “Ad Surf Daily,” “Ad Surf Daily Cash Generator,” “La Fuente Dinero” and “Golden Panda Ad Builder” (“ASD”). ASD represented itself as an Internet-based advertising company. On or about August 2008, the Secret Service seized 13 bank accounts containing over $40 million dollars in proceeds from the scheme. ASD took pains to avoid calling its members "investors," in an apparent effort to avoid

regulatory scrutiny. ASD promoted paid membership by claiming that its members could earn 125% of their membership fees. In addition, ASD paid commissions to existing members for referrals, apparently in order to encourage existing members to recruit new members. ASD's website claimed that fifty percent of each day's sales (membership fees paid by new members) was rebated to existing members. The other 50 percent was apparently kept by ASD for whatever it wished, be that administrative costs, advertising, or enrichment of ASD's promoters. On January 4, 2010, Judge Rosemary M. Collyer of the United States District Court for the District of Columbia issued a Default Judgment and Final Order of Forfeiture in this civil matter.

10. During the course of this task force investigation, it has become apparent that another auto-surf Ponzi scheme is operating that is, in all material aspects, no different from 12daily Pro, Phoenixsurf, and ASD. In fact, this entity began operating just weeks after ASD was put out of business by the Secret Service, and this new entity uses the same terminology and business model as ASD. This new entity calls itself either "iNetGlobal" or "inetsurf." It is hereinafter referred to as "iNetGlobal" and it is operated by Renner.

iNetGlobal

11. On Friday, January 8, 2010, Steven Keough, former CEO of iNetGlobal, contacted the U.S. Attorney's Office for the District of Minnesota regarding iNetGlobal and what Keough believed to be the questionable business practices of its owner/operator, Renner. Keough's educational background includes a Bachelor of Science in Chinese from the United States Naval Academy at Annapolis, Maryland; a Master of Arts in Congressional Studies from the Catholic University of America, Washington, D.C.; and a law degree from Boston College Law School. He has taken additional graduate classes in business, finance, and IT management from the University of Chicago's Graduate School of Business and Northwestern University's

Keller Graduate School of Management. He retired with the rank of Captain from the United States Navy, in which he served for twenty years on both active duty and in the reserves as a submarine officer and an Asian area officer. He is conversant in English, Chinese, and French. As a lawyer, he has worked primarily as an intellectual property specialist.

12. On or about January 11, 2010, your affiant received information from Keough regarding iNetGlobal's suspicious activities. Keough said he was concerned that large amounts of money were flowing through bank accounts related to iNetGlobal and that unusual system manipulation was being conducted by iNetGlobal's owner/operator Renner. Keough had recently been fired by Renner. Keough believed he had been fired because he continually questioned iNetGlobal's business practices.

13. Your affiant confirmed that iNetGlobal operates over the Internet at several websites, including http://www.inetglobal.com/public/index.php; http://www.inetglobal.com/inetsurf; and http://www.adpacs.com/index.html. Other websites associated with this Ponzi scheme include; http://v-mail.net/index.htm and http://www.cashcards.net/rep/99152/index.html. Each of these websites has been visited by your affiant, and on each, a Ponzi or rebate scheme of some sort was promoted. In addition, as described below in this affidavit, at the description of the conference in Flushing, New York, at paragraphs 63 through and including 69 below, the website http://www.v-local.com was offered to iNetGlobal members as a service they could sell.

14. According to the "iNetGlobal Advertising Terms of Service," published on the iNetGlobal website, "iNetGlobal is owned by our parent company Inter-Mark Corporation, incorporated in Nevada, USA." Investigation revealed that Renner appears to have filed or caused to be filed papers to incorporate Inter-Mark Corporation in Nevada, on August 31, 2006.

Renner is operating iNetGlobal and other businesses from 250 Second Avenue South, Suites 145 and 106A, Minneapolis, Minnesota.

15. Renner also operates other corporations. A search of the public records of Minnesota corporations, available on the Office of the Minnesota Secretary of State's website, revealed Renner appeared to have filed or caused to be filed papers to incorporate Cash Cards International, LLC ("CCI"), in Minneapolis, Minnesota, on or about March 19, 2001. Further, Renner appeared to have filed or caused to be filed papers to incorporate V-Record Entertainment, LLC ("VRE"), in Minneapolis, Minnesota, on or about April 26, 2004. According to the website, VRE is an inactive corporation. The Registered Office address for CCI and VRE is 250 Second Avenue South, Suite 110 (CCI) and 145 (VRE), Minneapolis, Minnesota. Renner also appeared to have filed or caused to be filed papers to incorporate V-Media Marketing, LLC and V-Media Development Corporation, in Minneapolis, Minnesota on or about September 25, 2008 (V-Media Development Corporation) and April, 10, 2008 (V-Media Marketing, LLC). There is also a registration of an assumed name of V-Media I on file with the Office of the Minnesota Secretary of State. The Registered Office for both V-Media Development Corporation and V-Media Marketing is 250 Second Avenue South, Suite 145, Minneapolis, Minnesota. Agents have learned that Renner owns and/or leases both of those suites. A search of the public records available on the Wisconsin Department of Financial Institutions website of Registered Corporations revealed Renner appeared to have filed or caused to be filed papers to incorporate Virtual Payment Systems, LLC ("VPS"), on or about February 3, 2006. Renner appears to have filed or caused to be filed papers to incorporate V-Webs, LLC on August 3, 2004, with a registered address of 250 Second Avenue South, Suite 145, Minneapolis, Minnesota. This appears to be an inactive corporation.

16. Between January 11, 2010 and January 29, 2010, federal agents logged on to the iNetGlobal website on multiple occasions and read:

a. The physical address for the "iNetglobal support center" is 250 Second Avenue South, Suite 106A, Minneapolis, Minnesota, 55401.

b. 'V-Local' has an address listed as 250 Second Avenue South, Suite 145, Minneapolis, Minnesota, 55401

c. On the website for "adpacs.com", the listed address for iNetglobal is 250 Second Avenue South, Suite 145, Minneapolis, Minnesota, 55401.

17. On January 29, 2010, my colleague, Senior Special Agent Robert MacQueen of the US Secret Service, was informed by the US Postal Inspection Service that all mail for Suite 145 at 250 Second Avenue South, Minneapolis, Minnesota is being delivered to Suite 106A within 250 Second Avenue South, Minneapolis, Minnesota, and that Intermark, Cash Cards International, and Renner all receive mail addressed to Suite 145, 250 Second Avenue South, Minneapolis, Minnesota.

18. On January 29, 2010 federal agents walked past the business entrances to Suites 145 and 106A at 250 Second Avenue South, Minneapolis, Minnesota. These suites open off a first-level internal corridor of this building, which is a mixed use building combining commercial offices and retail shops. By walking down an open flight of steps from the skyway level, one finds oneself in this corridor, which is open to the general public. Agents remained in the public skyway or public corridor at all times. From the hallway, through the windows, Agents saw business activity within Suites 106A and 145, specifically a seated receptionist answering the telephone, office workers typing on keyboards and passing hard copy documents among themselves, and office workers talking on the telephone. Agents saw signs reading "iNetGlobal"

and “V-Local.com” at the door of Suite 106A, and saw signs reading “V-Records” and “V-Webs” at the door of suite 145.

19. On January 26, 2010, Gittleman Association Management Corporation, which manages the building at 250 Second Avenue South, Minneapolis, Minnesota (the building is known as “Commerce at the Crossings”), provided, pursuant to subpoena, the following documents:

a. A spreadsheet identifying Suite 145 as being owned by “Cash Cards Int’l Steve Renner” and Suite 106 as being owned by MEDA company.

b. A document titled, “COMMERCE AT THE CROSSINGS ASSOCIATION, PROXY” which says that Suite 106 and Suite 106A are owned by MEDA Company.

c. A document titled “Resident Transaction Report”, which identifies Steve Renner, Cash Cards International, as the owner of 250 Second Avenue South, Suite 145.The document indicated Renner’s last payment of Association dues took place on January 8, 2010, and that this payment represented full payment of association dues by this particular association member for the month of January 2010 for Suite 145. The office suites in the building are condominiums, owned rather than rented, and the association dues are payments to the Business Condominium Association for the building.

d. A facsimile copy of a business check in the amount of $389.17, dated January 4, 2010, bearing a printed company name/address of Inter-Mark Corporation, 5348 Vegas Drive, Las Vegas, Nevada 89108. The check, , was drawn upon a Wells Fargo Bank branch in Boulder City, Nevada. The check was accepted by Gittleman Management Corporation as payment of “Business Condominium Association dues” for January 2010.

e. A facsimile copy of a business check in the amount of $351.99, dated August 26, 2009, bearing a printed company name and address of: CASH CARDS INTERNATIONAL, LLC, 250 2nd Ave, S. Suite 145, Minneapolis, MN 55401, payable to ‘Crossings Commercial Owners Association’. The check, ,was drawn upon a TCF of Minnesota account. The check was ittleman Management Corporation as payment of “Business Condominium Association dues” for September 2009.

f. A computer screen printout from Gittleman's internal property tracking software application (called "JenARK") listing "Steve Renner" as current owner of "250 2nd Avenue, South, 145".

20. Gittleman has advised SSA MacQueen that the various suites within 250 Second Avenue South, Minneapolis, Minnesota have been re-numbered three times. Gittleman advised SSA MacQueen that the suites within the building were "business condominiums," that is, Gittleman does not rent the suites out, rather the suites are owned, and Gittleman works for the "business condominium owners association." Although Gittleman does not have a separate account for a Suite 106A, only for Suite 106, Gittleman produced the proxy record referenced in subparagraph "b" above, showing that Suite 106 was subdivided by MEDA with the consent of the business condominium owners association. As noted above, the Postal Service indicates that all mail for Suite 145 (the owner of which is, as stated above, Steve Renner and Cash Cards International) is delivered to Suite 106A, signs at the door show Suite 106A to be occupied by iNetGlobal and V-Local.com., and a description and drawing of Suite 106A by Keough shows the suite to be occupied by iNetGlobal.

21. On January 28, 2010, during a follow-up interview with federal agents, Keough produced a hand-drawn sketch of his recollection of the physical space within Suite 145. The drawing produced by Keough was similar to the sketch of the same office space entered into evidence as Government Exhibit 54 at Renner's criminal tax evasion trial. Keough specified the last known work area locations of key, senior iNetGlobal employees who he expected would have knowledge of, or documents concerning, Renner's operation. Further, Keough provided specific direction as to where, within the space, he had previously directed staff members to store significant transactional / accounting documents. Keough stated these documents would be helpful in better understanding the operations of iNetGlobal and the other companies. Keough

produced a hand-drawn sketch of his recollection of the physical space within Suite 106A. Keough specified the last known work area locations of key senior iNetGlobal employees with possible knowledge and/or documentation of Renner's Ponzi operation. The sketches of both Suite 145 and Suite 106A appear reasonably accurate from public-area visual inspection/comparison - through window glass, during regular business hours. Keough stated he personally reviewed the incorporation paperwork applicable to Intermark Corporation (the 'umbrella' company) and that those documents showed Renner owned 100% of the shares of Intermark.

22. The datacenter for iNetGlobal is located at 77 13th Avenue Northeast, Suites 104 and 210, Minneapolis, Minnesota.

23. Agents performed a basic Internet search (WHOIS) for www.inetglobal.com. A WHOIS search gives the numerical Internet Protocol address on which a particular website is located on the Internet. The website does not actually occupy a particular physical space, but does occupy an addressable and uniquely identifiable electronic place on the Internet, and that electronic place is uniquely identified by the numbers that make up an Internet Protocol address. In this case, the WHOIS search for www.inetglobal.com showed that website to have an Internet Protocol address of 204.246.67.162. On January 25, 2010 agents conducted a standard internet routing search (TRACEROUTE) for that IP address. A TRACEROUTE search shows which server hosts a particular Internet Protocol address. The ownership of that server can then be researched. The numerical IP address 204.246.67.162 was found to be hosted by a server administered by Honeycomb Internet Services, located at 77 13th Avenue Northeast, Suite 210, Minneapolis, Minnesota.

24. A subpoena was served on Honeycomb Internet Services. On January 27, 2010

information obtained from Honeycomb Internet Services pursuant to that subpoena indicated that the servers which contain the IP address 204.246.67.162 are owned by "the best ISP" and that "the best ISP" is controlled by Theodore J. "Joe" Pound. Honeycomb Internet Services management specifically identified the physical machines owned by "the best isp / Joe Pound / iNetGlobal" to be within Honeycomb Internet Services company space, that is, within Suite 210. On January 29, 2010, Honeycomb Internet Services management said they were told by Joe Pound that he would be moving some equipment into a newly built-out business Suite on the floor below Honeycomb Internet Services (within the same building) and that a cable was to be connected from the computer equipment currently within Honeycomb Internet Services company workspace "down" to the newly established iNetglobal/Joe Pound/thebestisp workspace. This work was expected to take place later on the evening of January 29, 2010.

25. On February 1, 2010 Artspace Projects, Inc. advised via subpoena that their corporation owns the building known as 'Grain Belt Studios', 77 13th Avenue, Northeast, Minneapolis, Minnesota, 55413, and leases the property in the form of subdivided suites. Artspace Projects, Inc. provided documents which establish that iNetglobal and/or V-Media Marketing, whose points of contact are given as Theodore J. Pound and Steven M. Renner, lease Suite 104 and are currently occupying the space. Suite 104 is labeled "iNetglobal data center" on email correspondence provided by Artspace, Inc. personnel.

26. On February 3, 2010 Artspace Projects, Inc. provided via subpoena the floor plan of Suite 104 as agreed upon by iNetGlobal and Artspace, Inc. The floor plan clearly depicts the build-out for a datacenter with significant computer equipment. In particular, of the three rooms on the floor plan, one is labeled "datacenter." Another room, labeled "basement" shows three air conditioners (your affiant is aware from her training and experience that computers generate a lot

of heat and datacenters must be cooled to keep the computers from suffering harm due to buildup of heat) and a generator. The third room appears to be connected to the data center through a single door. The floor plan of the third room shows four desks, a counter, a conference room and an office.

27. Pursuant to subpoena, Steven Keough provided the following documents to federal agents on January 11, 2010:

A printed copy of an email from iNetGlobal employee Andrew Brager at e-mail address andy@inetglobal.com to Keough, dated December 2, 2009, and setting out information about a company called "the best isp" ("ISP" in the computer business, is an acronym for "internet service provider" which is a company that hosts internet services for businesses, organizations, and individuals). The Andrew Brager e-mail stated that Joe Pound (Theodore J. Pound) was the owner of "the best isp." The e-mail referred to "the best isp" as the historical internet hosting company for "all of Steve Renner's machines." The e-mail described 'the best isp' as now "own"(ed) by iNetGlobal, using "we" for iNetGlobal. Finally, the e-mail stated that "We also have some servers still hosted at the best isp…"

a. A printed copy of an email from Joe Pound, at e-mail address joe@thebestisp.com to Keough, dated November 16, 2009, discussing work space and structural requirements for a new data center.

A printed copy of an email from Keough to Beth Bowman at e-mail address \ beth.bowman@artspace.org , dated November 12, 2009, regarding an appointment to review the document (lease agreement) and walk through the proposed property site (Suite 104) with the

data center manager (Joe Pound). Keough also told agents that during an iNetGlobal Senior Staff meeting held on January 5, 2010, Joe Pound stated servers would be moved to the new location by the end of January, 2010.

28. The final location for which search warrant authority is sought is 411 Washington Avenue North, Suite 10, Minneapolis, Minnesota.

29. The web address http://www. inetsurf.com automatically redirects to the website http://www.inetglobal.com/inetsurf/. A basic Internet search (WHOIS) for that first web address shows it has an Internet Protocol address of 207.67.9.5. On January 25, 2010 agents conducted a standard internet routing search (TRACEROUTE) for Internet Protocol address 207.67.9.5. This numerical address is hosted by a server administered by Infotec, 411 Washington Avenue North, Minneapolis, MN, 55401. The contact person is given as Theodore Pound. Infotec in turn obtained the right to use this Internet Protocol address from TW Telecom, the owner of a large range of Internet Protocol addresses which includes 207.67.9.5.

30. On January 26, 2010, TW telecom returned subpoena information regarding the IP address of 207.67.9.5. TW telecom advised this IP address belonged to Infotec Company, 411 Washington Avenue North, Suite 10, Minneapolis, Minnesota, 55401 with a listed contact of Mr. Theodore Pound.

31. On January 29, 2010, a Secret Service Agent walked past the business doorways in the public area of this commercial building. Through an open doorway, the agent saw business activity within Suite 10, specifically, three men working around two desktop monitor systems. The agent also saw a sign reading “The Best ISP” posted at the door of Suite 10, 411 Washington Avenue North, Minneapolis, Minnesota. The agent went through the open doorway and asked the men for directions to another office in the building. While asking directions, the

agent, who has extensive training and experience in computer crime investigations, saw what he recognized as computer server stacks. Immediately upon receiving directions, the agent left.

32. On or about February 1 and 2, 2010, the same Secret Service Agent saw a dark red KIA Optima bearing Minnesota license plate in the parking lot of 411 Washington Avenue North, Minneapolis, Minnesota. This car, upon checking databases maintained by the Minnesota Department of Public Safety, Driver and Vehicle Services, was found to be registered to "Infotec Center / Theodore Joseph Pound".

Relationship Between Companies

33. According to a "Business Description For V-Media" obtained by Keough during his employment, "…V-Media primarily works for InterMark Corporation as a marketing firm. Through licensing agreements and marketing contracts, V-Media collects money throughout the year to conduct marketing for iNetGlobal, V-Local, V-Newswire, V-Webs, V-Shops, etc."

34. Virtual Payment Systems, LLC is considered part of, and the money transmitter for, Cash Cards International. According to an internal email "VPS is an LLC that is reported within Cash Cards." To further indicate this, when U.S. Secret Service Special Agent William Stack joined iNetGlobal in an undercover capacity (see paragraph 54, below), SA Stack was sent an invoice from Cash Cards International instructing him to wire payment to TCF account number in the name of "Virtual Payment Systems." The invoice also instructed SA Stack to put "For CCI purchase of V-Cash, CCI Invoice Number: " in the wire's memo section.

35. Customers buy various Internet services from InterMark. According to a power point entitled "Freedom Conference East – iNetGlobal Your Internet Solutions Partner", downloaded from iNetGlobal's website, and other documents obtained by Agents, the major

services that iNetGlobal claims to provide are web hosting, email auto-responders, web support, and advertising assistance. InterMark's customers are offered two options. When they purchase an Internet package (such as a "Consulting Kit" sold for $59.95), they can simply purchase that package or they can purchase the same package with the option of earning rebates and commissions (dependent on their continued participation in the InterMark community). If the customer purchases only the "Consulting Kit" (or variant of) without the possibility of earning rebates, then that customer is purely purchasing advertising services. A website owned by that customer will be placed on the so-called "rotator," that is, that customer's website will be clicked on by iNetGlobal members who are seeking to earn rebates. There is no price difference between a Consulting Kit with the possibility of rebates and a Consulting Kit without the possibility of rebates; both cost $59.95.

36. However, customers can purchase upgraded variants of Consulting Kits in order to increase their earnings potential. The names of the upgrades and their prices are as follows: $250 "Home Business Package," $500 "Small Business Package," $1,000 "Corporate Package," $2,000 "Executive Package," and $5,000 "Presidential Package".

37. Customers who seek to earn rebates from iNetGlobal are required to do so by use of InterMark's web service called "iNetSurf". Customers must also transact their financial dealing with iNetGlobal through another Renner company, Cash Cards International. The customer does not transact business primarily in currency, but rather, in "V-Credits," which are allegedly convertible to United States currency through Cash Cards International. V-Credits are sold by Cash Cards International.

38. According to a document entitled "Business Description for InterMark and Cash Cards International" provided by Keough, "iNetSurf requires the participants to browse through

a prompted group of web pages belonging to other InterMark customers. The reason for this is two-fold. First, the increased viewership of the members' websites increases the possibility of creating sales. Whether the members are selling products on their sites or encouraging advertisers to pay for space, the increased traffic is beneficial. Secondly, the sheer volume of views provided to members increases their sites' placement on major search engines like Google and Yahoo. (Generally, increased viewership convinces these search engines of the legitimacy of the sites)."

39. The Business Description also states that if a customer chooses not to participate in iNetSurf – that is, if a customer purchases just a Consulting Kit, without the possibility of earning rebates - there is no customer interaction with Cash Cards International and no utilization of V-Credits. However, if the customer chooses to participate in the rebate program, InterMark sends the customer's information to Cash Cards International and an account is set up so the customer can use V-Credits and eventually redeem those V-Credits for cash.

40. Once the customer begins viewing other member pages, rebates begin accruing. These rebates are not given out in the form of cash, but as "iPoints." Customers can then convert their "iPoints," to V-Credits stored by Cash Cards International, and finally, through Cash Cards International, convert their V-Credits to cash. Otherwise, they can keep the iPoints within the Inter-Mark system and purchase additional services. The V-credits are given to the customer directly from InterMark-thus, Intermark must first purchase them from Cash Cards. People who sign up with iNetGlobal but who are not earning rebates – so-called "free surfers" – are paid in the form of "iRewards" which are redeemable for merchandise sold through what is called the "iNetSurf Shop" or for Amazon.com gift cards. There are also other levels of participation, such as "preferred customer." All have their own method of reimbursement. No attempt is made here

to summarize all of them.

41. Still according to the Business Description, when Inter-Mark pays Cash Cards for V-credits, Cash Cards takes a percentage of the inbound wire transfer as a fee, books that fee to revenue, and holds the remainder in a Client Holdings Deposit account. Cash Cards can reconcile its Client Holdings Liability by comparing it to the total number of outstanding V-Credits, plus the customer balances requested out in the immediately preceding two weeks. InterMark's Rebate and Commission Liability should equal the current iCash Available Balance.

42. Finally, when a customer wants to 'cash out' their V-Credits, they send a request to Cash Cards International via iNetGlobal. They are given the option of receiving their money in the form of a check or wire transfer, or of having the funds loaded onto a Cash Card that they can use as an ATM Card to withdraw their cash. Cash Cards reduces its Client Holdings Liability, takes an outbound service fee, and returns the balance to the customer.

43. Agents have learned through internal memoranda that Cash Cards co-mingles its Clients Liability monies with its operations monies.

44. Agents have also learned that iNetGlobal's IT department is inadequate to fulfill these services. Keough reported that there is only one person assigned to assist those who are placing websites on the rotator. Keough reported that approximately 1000 customers had purchased the Consulting Kit without the option of earning rebates.. This represents a total of 1000 customers X $59.95 per customer = $59,950, which is not adequate to support the rebates and commissions that iNetGlobal promises it will pay its members.

45. iNetGlobal promotes memberships by claiming that its members can earn up to a 70% return.

46. Agents have also determined that most of the so-called advertisers are not paying

iNetGlobal for advertising services; instead, they are paying iNetGlobal with the expectation that iNetGlobal will provide a full rebate and additional revenue. Thus, absent continuous membership growth iNetGlobal has no means to generate the returns it represents that it will pay. Further details of the expectations of members joining iNetGlobal, and the numbers of them who do not have businesses that could benefit from iNetGlobal's advertising services, are set forth in the description of the conference in Flushing, New York, below at paragraphs 63 through and including 69, below. In addition, the fact that iNetGlobal depends upon member growth, not advertising revenue, to pay rebates to members is supported by the fact that the number of the sites on the rotator is much lower than the number of iNetGlobal customers. As noted below in paragraph 48 iNetGlobal has approximately 30,000 members; the number of sites on the rotator is frequently less than ten thousand.

Interview of former CEO Steven Keough

47. On or about January 11, 2010, agents conducted a voluntary interview with Keough. Keough stated that he had been hired by Renner as a consultant on or about October 27, 2009, to provide guidance in making the business grow. Keough now believes Renner believed Keough would be a "good face" for the company. According to Keough, Renner described iNetGlobal as an Internet-based company with two platforms, an Internet Service Provider (ISP) and a "Revenue Network" advertising application. Keough described what he called his first "red flags," which were the reported size (50,000 members) and purported revenue ($100 million) of iNetGlobal; the complete disarray and disorganization of the businesses; and the seemingly small outside legitimate income. Keough further stated that the companies' website never seemed to work properly, making him question what customers who purchased the advertising service alone, without the possibility of rebates, were getting for their

money. Keough said on occasion he witnessed Renner manually manipulating the iNetGlobal system to pay out percentages that were different, and smaller, from the percentage listed on the iNetGlobal website. Keough also wondered how, with so little outside income, the company could pay these outlandish returns. Keough said Renner would explain away his concerns by telling him how beneficial the advertising was and about all the different levels a member could achieve. Keough said, "I never really understood how it could work." Renner told him iNetGlobal had 50,000 members, had been in business for 10 years, was debt free, and had made over $100 million in revenue. Keough said he later learned all these facts were "lies." Keough further stated that Renner used the misleading information in power point presentations and webinars to recruit others.

48. On or about November 7, 2010, Renner hired Keough to be iNetGlobal's CEO. Once becoming CEO, Keough conducted his own internal audit and found, contrary to Renner's statements, that iNetGlobal had only approximately 30,000 members, iNetGlobal had only been in business for 14 months, there were huge liabilities associated with the members' "investments" and the company's estimated revenue was approximately $28 million, not the $100 million in revenue claimed by Renner. Keough said he was particularly alarmed because he knew Renner and/or representatives of iNetGlobal were using these false statements to promote and market iNetGlobal to would-be members (investors). Keough believed these false statements caused individuals to invest with iNetGlobal.

49. Keough said he had an iNetGlobal employee conduct an analysis to determine the member liability. The employee reported back to Keough that at least 87% of the company's revenue was generated from sale of memberships to members residing in China. All memberships include a certain number of "adpacs." An adpac is a purchase of a hit on your

website by another iNetGlobal member. If a member buys 500 adpacs, purportedly that member's website will be on the rotator until it has been clicked on 500 times by other iNetGlobal members, after which, unless the member has purchased additional adpacs, the member's website will be taken off the rotator. However, for individuals who are purchasing a membership but do not have a business or a website to promote on the rotator, the adpacs that are included in their membership become, from an economic point of view, simply a part of the price of the membership. Once this 87% of revenue was taken account of, only approximately 13% ($3.64 million) of the supposed $28 million in sales was left, originating from customers who purchased the Internet advertising package only, the Consultant Kit without the possibility of earning rebates. Keough said he investigated further and learned that the 13% figure could be far less, as the ISP platform which generated the "outside income" was not fully functional. Finally, Keough learned that the 13% figure he had been provided by the iNetGlobal employee was incorrect, because only approximately 1,000 members had signed up for Consultant Kits without rebate earning potential. This would constitute even less "outside income," approximately $60,000 (1,000 members x $59.95 consultant packet) or less than ¼ of 1 % of the overall revenue if overall revenue is equal to $28 million.

50. Keough described a typical incoming member transaction. A member purchases "adpacs" with a credit card. The credit card transaction is processed through a credit card processor called Anres Technologies, Inc.; Anres wires the proceeds, minus any applicable fees, to iNetGlobal's bank accounts. iNetGlobal then credits the member's account. Keough said iNetGlobal originally accepted wires and money orders but recently has migrated to accepting only credit card purchases. In order for a member to cash out, they could convert their iPoints to

V-Credits and then, through Cash Cards International, to dollars and receive a transfer of value to their debit card, receive a wire to their designated financial institution, or receive a check by mail.

51. Keough said he had received numerous complaints during the week of January 17 – 23, 2010 from members who could not convert their V-credits to cash and/or the website was not working properly. Keough said he told one member to "cash out" all of his monies to which the member replied that this was not possible due to the automatic "repurchase" feature set up within the iNetGlobal program. The automatic repurchasing feature is discussed fully below in this affidavit, at paragraph 51.

Steven Mark Renner

52. A check of the U.S. District Court, District of Minnesota, Electronic Document Filing System revealed four 2009 felony convictions for Renner, one each for four counts of tax evasion. The convictions were in the United States District Court for the District of Minnesota. According to court documents, Renner underreported his income by at least $1.5 million between 2002 and 2005 and owed more than $332,000 in tax as of 2006. Renner is currently awaiting sentencing in this matter.

53. A review of exhibits received during Renner's federal tax evasion trial, and discussions with the case agent, indicated that the jury heard testimony concerning difficulties with using the machinery of Cash Cards International to convert V-Credits into cash. In particular, in 2004, the United States Securities and Exchange Commission sued the operators of a Ponzi scheme called "Learn Waterhouse." This Ponzi scheme was headquartered in southern California, but used Cash Cards International to move funds. After the SEC filed suit, the United States District Court in San Diego appointed a receiver to seize, liquidate, and return to victims

any assets of Learn Waterhouse. The receiver contacted Renner, and asked for an "outconversion" (a conversion from V-Credits to cash) of all funds attributable to Learn Waterhouse held as V-Credits by Cash Cards International. This could not be done, as more than two and one-half million dollars of Learn Waterhouse V-Credits had been "invested" by Renner in stamps, coins, Salvador Dali sculptures, autographed letters, guitars and amplifiers, fractional interests in motion picture companies, and fractional interests in oil wells, among other things. Additional sums of customers' money had been spent by Renner personally, including on daily living expenses. Even when the investments were liquidated, the amount of money available to pay Learn Waterhouse victims was far short of the amount needed for a one-to-one conversion of V-Credits to United States dollars. In 2007, the receiver and Renner settled the matter of Cash Cards International's inability to make a full conversion of V-Credits to cash. In this settlement agreement, the receiver wrote off a substantial amount of funds that Renner was unable to convert from V-Credits to cash.

Federal Agents Join iNetGlobal

54. On or about January 14, 2010, US Secret Service Special Agent William Stack visited iNetGlobal's website, created a free "surfing" account with iNetGlobal, and began to visit its paid advertisements. SA Stack was directed to iNetGlobal's's own website's "News" section, to other sites promoting iNetGlobal, to sites promoting multi-level marketing programs generally, and to sites of individuals purportedly selling services, such as weight loss. SA Stack attempted to sign up as a "consultant." The registration for "consultant" was locked until the "Consultant Kit" was purchased for $59.95. Then, SA Stack attempted to register as a "Preferred Customer", but was unsuccessful. It appeared that one first had to purchase "adpacs" in an amount of $20, $50, $100, $250, $500, or $1,000 before continuing with the registration. SA

Stack attempted to complete registration, but the website iNetGlobal.com had a message stating the web servers were down for maintenance and so SA Stack was unable to access the website. Approximately three hours later, SA Stack again attempted to register after the website was back online and was successful in creating a "free surfer" account. SA Stack received an email from iNetGlobal, describing itself as a division of Inter-Mark Corporation, 5348 Vegas Drive, Las Vegas, Nevada 89108, welcoming him as an "elite member of Internet Marketers," and providing a new iNetGlobal login and password. SA Stack then received another email from iNetGlobal. In answer to a question posed to him in that e-mail he responded "Yes- I do not have a sponsor and would like the company to assign one to me." All of this was done through a Secret Service undercover email account. After successful login, SA Stack signed up for "V-Cash". SA Stack received an email from Cash Cards International which provided a link to "The Cash Cards – iNetGlobal Portal Members Center" with a Member ID Number and Password. SA Stack clicked the link and was directed to www.cashcards.net/group/ iNetGlobal. SA Stack requested $1,000.00 worth of V-Cash Credits and received an invoice via email to an undercover email account. The invoice for $1,000.00 worth of V-Cash Credits includes a $40.00 funding fee for wire orders. The invoice also included the bank wire information for Virtual Payment Systems, TCF Bank Account# . The invoice also had information needed to complete an InExchange Authorization Document which was addressed to Cash Cards Hawaii, LLC. SA Stack logged in to iNetGlobal and began to visit its paid advertisements. The website advertisements ran below the 20 second timer within the iNetGlobal website (surf.inetglobal.com/surf.php) and ranged from other multi-level marketing sites to affiliate programs, non-English websites, and even iNetGlobal's home page.

Few Legitimate Advertisers

55. On or about January 15, 2010, Secret Service SA Roy Dotson had a telephone conversation with an iNetGlobal member. Agents identified this member through a Google search for iNetGlobal. The member had a personal website promoting iNetGlobal and other multi-level marketing programs. The member asked if SA Dotson was a network marketer. The member said he had previously been a member of ASD (AdSurf Daily, described in paragraph nine above in this affidavit) and said, "We know what happened there." The member said he was reluctant to join iNetGlobal due to it being similar to ASD. The member said, "we all know what this program is." The member said his daughter and wife surfed the websites and the member did not care about the services provided. The member said he just wanted to put his money in and get it out. The member said you convert your earnings to V-cash and then receive payouts by check or through an ATM card you can sign up for. The member said members earn a daily return on their investment but that he was not sure what he exactly earned. The member said he has not been able to figure out the percentage of return due to the convoluted information provided on the iNetGlobal website. The member said he believed it was a little less than one half percent a day. The member was critical of the job iNetGlobal did of marketing itself. The member pushed SA Dotson to join and wanted to conduct a three way call with his sponsor. The member said bringing in new members under you was the best way to earn maximum returns.

Rebates Paid Even When No Ads Viewed

56. iNetGlobal pays daily rebates (purportedly earned by viewing advertising on the rotator) even on dates when iNetGlobal's webpage is inaccessible and so no advertising can be viewed. This investigation has revealed that the iNetGlobal website regularly is down and/or not functioning. Former CEO Keough stated all active members received daily payouts regardless of surfing activity. Keough said he had witnessed Renner manually manipulating the daily

percentage of return due to, among other things, the system being down and members being unable to surf. This is in direct opposition to iNetGlobal's Terms and Conditions which state, "If an Advertiser misses a day of viewing the required number of web sites, he will not earn any rebates for that day only". Your affiant has used the free surfer account on iNetGlobal created by SA Stack. Attached is a screen shot showing a message to members stating "every member" will earn credit for surfing on January 30 and 31, and February 1, apparently without regard to whether the member surfs the web on those days.

FTC Opinion

57. In addition to reviewing materials available from the SEC, during the course of this investigation Agents consulted with an Economist, Kenneth Kelly, at the Federal Trade Commission (FTC) who explained that pyramid or Ponzi schemes are all schemes where the participants obtain their monetary benefits primarily from the recruitment of new participants, rather than from the sale of goods or services. Because of this, the overwhelming majority of the participants cannot expect to make any money from their participation. A small minority of participants, namely those who participate at the very beginning, might make money. However, because of the nature of the pyramid scheme, those who make any money must of necessity be only a small minority of all participants.

58. Economist Kelly further explained that growth of a Ponzi scheme does not change the fact that the large majority of participants at any point in time will have lost money. The system cannot grow indefinitely, if for no other reason than the fact that growth is limited by the finite human population of the earth. But long before this point is reached, the number of people willing to pay to sign on as new participants will become fewer and fewer. At this point, no further growth is possible, and the scheme will collapse. When that happens, the majority of the

participants will have lost money.

59. Economist Kelly further explained that these scams typically have one of several indicators or "markings," including (1) the promise of abnormally high short term returns on investments; (2) all income is derived from within the investment scheme; (3) the absence of any legitimate or reasonable business investment; and (4), as described above, only a small minority of individuals can profit from the operation of the business. When Agents described the details of iNetGlobal to the economist, he indicated that iNetGlobal bore all of the characteristics of a Ponzi operation.

Customer Complaints

60. On or about January 12, 2010, Agents received information from former iNetGlobal CEO Keough regarding a victim in the state of Nevada. According to Keough, a high level iNetGlobal member contacted him on January 11, 2010, complaining that for over one week they had been unable to get a money order payment from the company for value they are owed. The victim contacted iNetGlobal's customer service on several occasions only to get excuses. The victim asked Keough what he should do and Keough told him/her to cash out of the system and the victim said, "We can't cash out, it is not possible, due to mandatory repurchasing built into the system."

61. Your affiant logged on to the iNetGlobal website on February 1, 2010. Your affiant was logged in as a free surfer. "Automatic repurchasing" was enabled by default. When this feature is enabled, a certain portion of what one earns through viewing of advertising is plowed back into the company. The percentage that is put back into the company can be no lower than 40 percent and goes all the way up to 100 percent. Your affiant turned the automatic repurchasing feature off manually, but each time your affiant did so, it came back on. A

disclaimer on the web page stated that "Executives" had to enroll in automatic repurchasing. As noted, your affiant was logged in as a free surfer. Your affiant has attempted to disable the automatic repurchase several times on different days. Your affiant has never succeeded in disabling the automatic repurchase feature. Nor has your affiant ever succeeded in setting the automatic repurchasing percentage at zero, or indeed, at any percentage lower than 40 percent. On February 17, 2010 your affiant sent an e-mail inquiry to iNetGlobal customer service asking if automatic repurchasing could be turned off. Customer service replied in the negative.

62. In addition to the complaint from the high level member described in the preceding paragraph, numerous complaints have been received by iNetGlobal customer service regarding the website not functioning properly. According to former CEO Keough, customer service was inundated with phone calls from members complaining that the website never worked properly.

iNetGlobal "Freedom Conference 2010" in Flushing, New York

63. On January 23, 2010, your affiant and US Secret Service Special Agent Roy Dotson traveled to Flushing, New York, and attended the iNetGlobal "Freedom Conference 2010." This conference was held in a hotel conference facility. The segments of the conference attended by Secret Service agents were free and open to the public.

64. Approximately 400 people attended the conference. The majority were Chinese. Those attendees to whom your affiant spoke had either little or no facility in English. In addition, your affiant observed that conference registration took a long time because nobody at the registration desk spoke Chinese, and many of the conference attendees could not make themselves understood in English. There was an interpreter in the main hall, but Renner often spoke over the interpreter. Renner began the conference by asking the attendees "who wouldn't

want to put ten dollars in and get twenty back?" He removed a large amount of cash from his pocket and held up twenty dollar bills, which he began handing out to attendees in exchange for ten dollar bills. This caused a crush of people to approach the front of the hall, and Renner eventually needed assistance moving people back. Renner asked, through an interpreter, how many people in attendance had their own business, and only two raised their hands. SA Dotson followed up on this point by approaching Kathy Zhang, who had been identified by Renner as a New Jersey resident making $6,000 per day, or $180,000 per month, with iNetGlobal. SA Dotson asked Ms. Zhang if she had a website of her own, and Ms. Zhang replied no, that was not required. SA Dotson also approached Gang Li Guo, who told SA Dotson he had made about $3000 per month. SA Dotson asked Mr. Guo if he had a website to advertise on iNetGlobal, and Mr. Guo said he did not. He had a website, but because it was ten years old, Mr. Guo did not post it.

65. SA Dotson overheard an individual ask Renner if they invested $2000 and did nothing but surf, how long would it take to earn back their money to which Renner replied that in four months the member would get their money back plus an additional two hundred. Renner did not talk to the potential member about advertising or the need for a website or a business.

66. Renner at various times stated that he had made over $65 million in various Internet businesses; that iNetGlobal had been in business for ten years, and that it had an aggregate of over $100 million in revenue, $25 million of that coming in December of 2009 alone. A short time later, Renner stated that iNetGlobal had $20 million in sales in December of 2009. Renner stated that iNetGlobal's search engine, Access, would soon rival Google's. Renner did not explain to the crowd that Access was simply a link to another search engine, and that an Access web search was just the same as a web search on this other search engine. Internal

e-mails discuss the possibility of the other search engine cutting the link and thus taking down Access. Keough also confirmed that Access simply links to another search engine.

67. Renner claimed that iNetGlobal's business directory, V-Local, had over 3.5 million businesses signed up. He explained that attendees could make a great deal of money selling V-Local and signing up businesses to participate in V-Local. Renner stated that V-Local was expanding into Canada, Europe, and China. He claimed that when a company was listed on V-Local, iNetGlobal would list the business with over 65 local directories, plus social networking sites, and would arrange for the business to be input into Garmin and TomTom GPS navigation devices, as well as Cadillac OnStar. On January 28, 2010, your affiant searched for "coffee shop" in Minneapolis, Minnesota on V-Local, asking V-Local to find the nearest coffee shop. There were no results. Your affiant then broadened the search to coffee shop, food and dining. V-Local then identified six coffee shops in Iowa, Kansas, and other states, only one of them in Minnesota (in Byron). Renner stated that if an attendee wanted to sell V-Local the attendee would need to pay $300, watch several videos, and take a certification test. Renner stated that for every person in a member's "downline" who got certified to sell V-Local, the original member would receive $100. Renner stated that this would be an enormous jump in a member's income. Approximately one week after the Freedom Conference, your affiant searched on V-Local for "gym" and "restaurant." There were no hits in the search for gym, and only one hit in the search for restaurant.

68. While SA Dotson was attending the main meeting, your affiant went across the hall to the "Opportunity Meeting." This was hosted by iNetGlobal employee Steve Allen, International Marketing Director for English-Speaking Countries. Allen began by stating that no results were guaranteed.

69. Your affiant listened while a person talked to Donald Allen about iNetGlobal. Donald Allen is also an employee of iNetGlobal (and is not the same person as Steve Allen). The person stated she was struggling to understand how the business worked and explained that the person who brought her to the conference was not able to explain it either. She asked what would happen if she sold iNetGlobal products to someone who had a website and they did not see an increase in their profits. Donald Allen asked her what type of products the person was selling and the woman gave the example of beauty products. Donald Allen replied that if she was advertising beauty products and not selling any, then maybe she should be in a different business. The woman further challenged Donald Allen on people not truly viewing the websites, just simply opening them. Patricio Diez, iNetGlobal's marketing director for Spanish-speaking countries, then stated that "that doesn't matter for you". When the woman pressed further, stating that it does matter to whomever she sold the package to, Donald Allen simply stated "we have solutions for that" but failed to expand upon those solutions**.**

Use of Interstate Wire Communications

70. As noted above at paragraph one of this affidavit, your affiant has extensive training in computer crimes, and also has substantial experience in investigating crimes whose commission is facilitated by the use of the Internet. Based on your affiant's training and experience, your affiant knows that use of the Internet necessarily involves use of interstate wire communications. This is because of the very structure of the Internet. The Internet is a network; messages, including e-mails, are sent over the Internet by being broken up into smaller packets that are then reassembled at the receiving end. Each of these packets is sent via whichever electronic route is least congested at the precise instant the packet is sent. This means (a) that each packet might take its own route, different from the routes of all the other packets of which

the email in question is composed, from origin to destination, and (b) that the least congested route in any given case might take the packet across multiple state lines and even international frontiers. Even an e-mail message that is going across town might, in the course of its disassembly, transmission, and reassembly, involve transmission facilities in several different states. In addition to this, as noted in this affidavit at paragraph 60 and paragraph 64, the activity in this case has included web surfing by iNetGlobal members from Nevada and New Jersey, who do their web surfing via computers hosted on servers based in the Twin Cities.

Banking Activity

71. Once funds are received by iNetGlobal they frequently move through a series of bank accounts. A review of the documents obtained and other investigation revealed the following bank accounts;

a. Wells Fargo account number , bearing the name Inter-Mark, and identified as a payroll account by Keough.

b. Wells Fargo account number , bearing the name Inter-Mark, and identified as a savings account by Keough.

c. Wells Fargo account number , bearing the name Inter-Mark, and identified as an ope unt by Keough.

d. Wells Fargo account number , bearing the name Inter-Mark, and identified as an inb ccount by Keough.

e. Wells Fargo account number , bearing the name Inter-Mark, and identified as an inbound credit card account by Keough.

f. Bremer Bank, account number , bearing the name Virtual Payment Systems.

g. Bremer Bank account number bearing the name of Cash Cards International LLC.

h. Bremer Bank account number bearing the name of Virtual Payment Systems, LLC.

i. Bremer Bank account number bearing the name of V-Media Marketing, LLC.

j. TCF account number bearing the name Virtual Payment Systems, LLC, and id n inbound wire account by Keough.

k. TCF account number bearing the name Virtual Payment Systems, LLC, and id "cash out" account by Keough.

l. TCF account number bearing the name Cash Cards International LLC, and identified as an operations account by Keough.

m. TCF account number bearing the name V-Records Entertainment LLC, and identified as an operations account by Keough.

n. TCF account number bearing the name of Cash Cards International LLC, and identified as a payroll account by Keough.

o. TCF account number bearing the name of Steven Mark Renner.

72. Analysis of the documents pertaining to the accounts revealed the following:

a. During 2009 funds were deposited into WF account number (inbound credit card) from credit card processors for iNetGlobal.com, V-Media Marketing and Inter-Mark. Some of these funds were transferred via online transactions to WF account number (operations), from which numerous withdrawals at various branch banks were made.

b. On January 7, 2010 an online transfer was made from WF account number (inbound credit card) to WF account number (saviNetGlobals) in the amount of $1,000,000.

c. On June 17, 2009 an online transfer was made from WF account number (inbound credit card) to WF account number (inbound wire) in the amount of $280,000.

d. On November 6, 2009 a transfer was made from WF account number (payroll) to WF account number (savings) in f $450,000.

e. On November 3, 2009 a credit was made from WF account (operations) to TCF account (cash out) in the amount of $300,000.

f. On September 10, 2009, September 24, 2009, and September 26, 2009 h in the amount of $2,500. e from TCF account (cash out) to TCF account (operations).

g. On March 26, 2009, $1,329.51 was withdrawn, via automatic withdrawal, from TCF account (operations) to "V Records Enter" via direct deposit

h. On April 30, 2009 $1,840.84 was withdrawn, via automatic withdrawal, from TCF account to "V Records Enter" via direct deposit.

i. On June 4, 2009 , 2009 transfers were made from TCF account number (operations) to TCF account (payroll) in the a ,500.

j. On June 2, 2009 and June 18, 2009 transfers were made from TCF account number (cash out) to TCF account (operations).

k. On May 19, 2009 a transfer was made for $1,000 from TCF account number (operations) to TCF account number .

l. On September 10, 2009, September 20, 2009, and September 28, 2009, transfers were made for $1,000 from TCF account number cash out) to TCF account number .

m. On December 23, 2009 a transfer was made from TCF account number to TCF account number (operations).

n. On January 14, 2010, SA Stack, while acting in an undercover capacity, signed up for a "free surfer" account. When SA Stack requested 1,000 V-Credits, the invoice included the bank w ion for Virtual Payment Systems TCF Bank Account# .

73. On January 20, 2010, Agents received information from a TCF National Bank investigator about the closing of accounts used and/or under the control of the InterMark Corporation, its subsidiaries or agents. TCF Bank had given notice to Renner that the accounts were going to be closed because of the bank's suspicions that the activity in the accounts might be money laundering. According to the bank investigator, an employee of NetGlobal named

Amy Ayd came into the bank on January 20, 2010 at approximately 9:00 AM and closed six InterMark-associated accounts. The following accounts were closed: in the name of Virtual Payment Systems, LLC; in the name of Virtual Payment Systems, LLC; in the name of Cash Cards International, LLC; in the name of Cash Cards International, LLC; in the name of V-Records Entertainment, LLC and in the name of Steven Mark Renner. Ayd received a cashier's check for a little over $5 million for the balances in the accounts. Per the bank investigator, the cashier's check could be deposited into new or existing accounts at any financial institutions.

74. On the same date, Agents received information from a Bremer Bank employee that around 12:00 noon, approximately $5 million was deposited into the four aforementioned Bremer Bank accounts. The deposits all came from a TCF bank issued check bearing the name of Amy Ayd.

Search Methodology - Computers

75. Because this warrant requests permission to search any seized computers or computer-related materials as defined below, specially-trained Secret Service computer forensics personnel, specially trained in the retrieval of information from computers, will participate in the execution of these warrants. It is believed the computers will contain both evidence of criminal activity, as well as be an instrumentality of the crime itself.

76. Searching computerized information for evidence of crime commonly requires the conservation of most of the computer hardware, software, documentation, and data security devices (including passwords and encryption keys) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. The analysis of electronically stored data, whether performed on-site or in a laboratory or other

controlled environment, may entail any or all of several different techniques. Such techniques may include, but not necessarily be limited to, surveying various file "directories" and the individual files they contain; "opening" or reading the first few "pages" of files in order to determine their precise contents; skimming the remainder of files in order to ensure nothing relevant is contained within an apparently irrelevant file, "scanning" storage areas to discover and possibly recover recently deleted data; "scanning" storage areas for deliberately hidden files; or performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation. This is true because of the following:

a. The volume of evidence: Computer storage devices (like hard disks, diskettes, tapes, thumb/flash drive, laser disks, Jaz, Zip and Bernoulli drives) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored.

b. Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted

files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap") a controlled environment is essential to its complete and accurate analysis.

c. Data analysis may use several different techniques to search electronic data for evidence or instrumentalities of a crime. These include, but are not limited to the following: examining file directories and subdirectories for the lists of files they contain, "opening" or reading the first few "pages" of a selected files to determine their contents, scanning for deleted or hidden data, searching for key words or phrases ("string searches").

77. In view of the foregoing, your Affiant seeks permission to search:

a. Any and all computer hardware, software, documentation, electronically stored data, and passwords and data security contained within any computer or computer-related materials seized, as described below.

i. “Hardware” - Computer hardware consists of any and all computer equipment capable of being linked together in a local area network (LAN) (this includes any equipment which has remote access capabilities) including all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives/flash drives, compact flash cards, tape drives and tapes, optical storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communication devices (such as modems, cables and connections); as well as any

devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

ii. “Software” - Computer software is digital information which can be interpreted by a computer and any related components to direct the way they work. Software is stored in electronic, magnetic, optical, or digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

iii. “Documentation” - Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

iv. “Electronically Stored Data” - Any and all such data concerning the crimes of wire fraud and money laundering, as more fully described in the balance of this affidavit. This includes information stored on back-up tapes, on computer hard drives, and/or any other form or manner.

v. “Passwords and Data Security” - Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming codes. A password (a string of keyboard characters) usually operates as a sort of digital key to "unlock" particular data security devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

78. As a result of the foregoing, the Court's permission is requested to seize, if necessary, the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the "List of Items To Be Seized." The Secret Service wishes to "image" the storage devices described in the "hardware" sub-paragraph above (sub-paragraph (a)(i)). An image of an electronic storage device is an exact copy, down to the binary ones and zeros of the information stored on the device, of that device. The Secret Service will undertake all possible efforts to do this imaging on-site, in order to minimize any disruption of legitimate business activities that removal of the devices for imaging might cause. However, the amount of electronic media, technical issues, encrypted data and unique equipment/software that may be found may make onsite imaging impossible. It will be the Secret Service's objective to find and seize the items in the "list of items to be seized" in the least obtrusive manner possible, including on-site imaging if practicable, while insuring the acquisition of the evidence for which this warrant has been issued.

79. Appropriately trained personnel will search any computers, along with any computer related equipment, including peripheral hardware or software or security devices, for any evidence of the Ponzi scheme described in the foregoing paragraphs. If, after inspecting the input/output peripheral devices, system software, and pertinent computer related documentation, it becomes apparent that these items are no longer necessary to retrieve and preserve the evidence – and are not an instrumentality of a crime -- such materials and/or equipment will be returned within a reasonable time. If off-site imaging and testing is necessary, it will be conducted expeditiously and once the images have been verified as usable, the seized items will be returned to the respective owners.

80. Your affiant is requesting authority to search for and seize items dated beginning

July 1, 2008. Your affiant has reviewed bank statements and other bank documents that concern the various accounts held by Intermark, and has noted that the balances in those accounts begin moving up sharply in August 2008.

81. Based on the information provided in this affidavit, your affiant respectfully submits that there is probable cause to believe that iNetGlobal, Steven Mark Renner, and others, have devised and intended to devise a scheme or artifice to defraud, or a scheme for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, and that he and they transmitted or cause to be transmitted by means of wire communications in interstate or foreign commerce, (including writings, signs, signals, pictures, or sounds) for the purpose of executing such scheme or artifice, to wit: an Internet-based Ponzi scheme, in violation of Title 18, United States Code, Section 1343 (Wire Fraud). Further, there is probable cause to believe that Renner conducted "monetary transactions" in amounts greater than $10,000, with the proceeds of specified unlawful activity, namely wire fraud, in violation of Title 18, United States Code, Section 1343, and that the conduct of these transactions constituted money laundering, in violation of Title 18, United States Code, Section 1957. Your affiant respectfully submits that there is probable cause to believe that fruits, instrumentalities, and evidence of the

commission of these crimes, as specified on the attached list of items to be seized, will be found at the places for which search warrant authority is sought.

_____
KatherineWespetal
Special Agent, United States Secret Service

Subscribed and sworn to before me

this _____ day of February 2010,

_____
Donovan W. Frank
Judge of District Court
District of Minnesota